UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF NEW YORK

EDWARD KOELLER and KEVIN CHEEK, individually and on behalf of all others similarly situated, Plaintiffs, v. NUMRICH GUN PARTS CORPORATION, Defendant.	Case No. 1:22-cv-00675-DNH-CFH **SECOND AMENDED CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiffs, Edward Koeller and Kevin Cheek ("Plaintiffs"), file this Second Amended Class Action Complaint on behalf of themselves, and all others similarly situated against the Defendant, Numrich Gun Parts Corporation ("Numrich" or "Defendant"), and its present, former, or future direct and indirect parent companies, subsidiaries, affiliates, agents, and/or other related entities. On personal knowledge of their own circumstances and upon investigation and information and belief of their counsel, Plaintiffs allege the following:

INTRODUCTION

1. Numrich, a firearm parts and weapons retailer, lost control over at least 45,169 of its e-commerce customers' highly sensitive personal and financial information in a data breach by cybercriminals ("Data Breach"). That information included their names, addresses, and payment card information, including card number, security code, and expiration date.

2. Class members are already reporting rampant fraud, as the breach involved all the card information necessary to fraudulently charge their accounts. As a result, consumers, including Plaintiffs, are devoting time and resources to prevent fraud on their accounts, cancel cards, monitor

for charges, and mitigate their damages.

3. But the risk for harm does not stop there, nor can Plaintiffs and the Class eliminate the risk by merely closing their affected accounts. Indeed, Numrich's breach is especially dangerous because it poses a threat to Plaintiffs' and the Class's physical safety.

4. The threat arises from the products that Numrich sells and the data it collects on customers to facilitate those sales.

5. Numrich sells gun parts that replace and modify the components for dangerous weapons, including bayonets and scabbards, gun magazines, stocks, suppressers, muzzle brakes and gun sights and components. In so doing, Numrich holds itself out as the "World's Largest Supplier of Gun parts" capable of "supplying the parts that fix, restore, improve, and complete every gun, regardless of when or where it was made."[1]

6. In other words, Numrich does not only cater to everyday gun purchasers, but also to gun enthusiasts and collectors.

7. Those purchasers, enthusiasts, and collectors value their privacy, including the sensitive nature of owning guns and dangerous weapons. As the Federal Bureau of Investigation reported, from 2012 to 2017, nearly more than $829 million worth of guns were reported stolen from individuals nationwide, amounting to an estimated 1.8 million guns.[2] Once stolen, those guns "pose a significant risk to community safety."

8. In fact, criminals *target* individuals they know own firearms because the firearms

[1] *See* Numrich's "About" page at https://www.gunpartscorp.com/about (last visited October 20, 2022).

[2] *See* Center for American Progress's State-by-State report on "Stolen Guns in America" at https://www.americanprogress.org/article/stolen-guns-america/ (last visited Oct. 20, 2022).

have value they can trade on.[3]

9. Thus, Numrich's Data Breach has exposed Plaintiffs and the Class to two risks for theft; just as hackers can misuse the data they stole in the Data Breach to steal money from Plaintiffs and the class, they can use their information to target them for theft at their homes.

10. Indeed, the criminals who stole customers' information now know that Plaintiffs and the Class own firearms and where they live, threatening their safety. As one data security website reported, "Gun ownership is a sensitive topic in itself, so identifying large firearms purchases could put customers in the crosshairs of criminals who are on the lookout for valuable stashes."[4]

11. Plaintiffs' and the Class's losses and threats to their safety are due to Numrich's inadequate cybersecurity policies and systems.

12. On or around March 28, 2022, Numrich became aware of suspicious activity on its e-commerce website, www.gunpartscorp.com. Numrich's investigations revealed that hackers gained unauthorized access to customers' confidential personal information and their payment card data (together "PCD"). The Data Breach occurred between January 23, 2022, and April 5, 2022 (the "Breach Period").

13. On information and belief, hackers gained unauthorized access to Numrich customers' PCD who made purchases through the website during the Breach Period.

14. Numrich electronically collects and stores its online customers' payment card information after each purchase—holding within its systems a treasure trove of useful information attractive for hackers who can use the payment data to make fraudulent purchases and cause real

---

[3] *Id*.

[4] *See* BleepingComputer's article *Online gun shops in the US hacked to steal credit cards* at https://www.bleepingcomputer.com/news/security/online-gun-shops-in-the-us-hacked-to-steal-credit-cards/ (last visited October 20, 2022).

substantial damage to consumers. Criminals may also use the information to target gun owners for

15. On information and belief, Numrich placed its personal financial gains ahead of its customers' interests and refused to shut down e-commerce through its website, even after discovering the Data Breach and prior to providing any type of notice about the breach.

16. On information and belief, the stolen PCD included, at least, customers' names, addresses, payment card numbers, card security codes, and expiration dates.

17. On information and belief, cybercriminals were able to breach Numrich's website and system because Numrich did not maintain reasonable security safeguards or protocols to protect its customers' PCD, leaving it an unguarded target for theft and misuse.

18. On information and belief, the Data Breach was undetected for over two months.

19. On or around June 6, 2022—over two months after discovering the breach and nearly five months after the start of the breach—Numrich began to notify breach victims that their PCD was compromised (the "Breach Notice").

20. When Numrich finally announced the Data Breach, it deliberately underplayed the breach's severity and misrepresented that it was "unaware of any actual misuse of information related to [the breach,]" even though Numrich knew cybercriminals had infiltrated its website and data for months. Numrich's Breach Notice obfuscated the nature of the breach and the threat it posed—refusing to tell its customers how many people were impacted, how the breach happened, or why it took over two months for Numrich to send a bare-bones notice. A true and correct copy of the Breach Notice is attached hereto as **Exhibit A**.[5]

21. Numrich's failure to safeguard customers' PCD and adequately warn them about

[5] Breach Notice obtained from the website of the office of the Maine Attorney General, https://apps.web.maine.gov/online/aeviewer/ME/40/c85b1a09-ea9b-4402-abb0-4d404f02d730.shtml (last visited June 15, 2022).

the Data Breach violates New York and Missouri law, harming thousands of individuals. Plaintiffs received Numrich's Breach Notice and are Data Breach victims, causing them to seek relief on a class wide basis.

22. Numrich knew or should have known that each victim of the Data Breach deserved prompt and efficient notice of the Data Breach and assistance in mitigating the effects of the breach.

23. Numrich's misconduct has injured the Plaintiffs and members of the proposed Class, including: (i) costs associated with the prevention, detection, and recovery from fraudulent charges, and other unauthorized use of their data; (ii) lost opportunity costs to mitigate the Data Breach's consequences, including lost time; (iii) lost benefit of their bargain, as they would not have purchased products from Numrich had they known it would not adequately protect their data; and (iv) emotional distress associated with the loss of control over their PCD and the threat it poses to their safety.

24. Plaintiffs and members of the proposed Class are victims of Defendant's negligence and inadequate data security measures. Specifically, Plaintiffs and members of the proposed Class trusted Defendant with their PCD. But Defendant betrayed that trust. Defendant failed to properly use up-to-date security practices to prevent the Data Breach.

25. On information and belief, the customer information and PCD compromised in the Data Breach is still stored in Numrich's online systems, Plaintiffs and members of the proposed Class have an interest in ensuring that their information is safe, and they should be entitled to seek injunctive and other equitable relief, including independent oversight of Numrich's security system.

26. Plaintiffs and members of the proposed Class therefore bring this lawsuit seeking

damages and relief for Defendant's actions.

PARTIES

27. Plaintiff, Edward Koeller, is a natural person and adult citizen of Missouri. Mr. Koeller intends to remain domiciled in Missouri indefinitely, and maintains his true, fixed, and permanent home in Missouri. Mr. Koeller has been a Numrich customer since September 2015 and is a Data Breach victim, receiving Numrich's Breach Notice in June 2022.

28. Plaintiff, Kevin Cheek, is a natural person and adult citizen of South Carolina. Mr. Cheek intends to remain domiciled in South Carolina indefinitely, and maintains his true, fixed, and permanent home in South Carolina. Mr. Cheek has been a Numrich customer since approximately 2017 and is a Data Breach victim, receiving Numrich's Breach Notice in approximately June 2022.Defendant, Numrich Gun Parts Corporation, is a New York Corporation, with its principal place of business at 226 Williams Lane, Kingston, NY, 12401.

JURISDICTION & VENUE

29. This Court has subject matter jurisdiction over this action under 28 U.S.C.§ 1332(d) because this is a class action wherein the amount in controversy exceeds the sum or value of $5,000,000, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one member of the class is a citizen of a state different from Defendant, establishing minimal diversity.

30. This Court has personal jurisdiction over Defendant because it is incorporated in New York and its corporate headquarters is in Kingston, New York.

31. Venue is proper in this Court under 28 U.S.C.§ 1391 because a substantial part of the alleged wrongful conduct and events giving rise to the claims occurred in this District and because Defendant conducts significant business in this District.

BACKGROUND FACTS

a. Numrich's Failure to Prevent the Data Breach

32. Plaintiffs and members of the proposed Class are Numrich's former and current online customers.

33. To complete online transactions, Numrich requires its customers to enter their payment card and personal information in order to receive the firearms parts being purchased.

34. When Numrich collects this sensitive information, it promises to use reasonable measures to safeguard the PCD from theft and misuse.

35. In fact, Numrich informs its online customers that it collects and maintains their PCD through the Privacy Policy (the "Privacy Policy").[6] A true and correct copy of the Privacy Policy is attached hereto as **Exhibit B**.

36. The Privacy Policy warrants that the privacy of its customers is "important" to Numrich. Indeed, Numrich asserts that it "does not sell, trade, or share [customers'] information with anybody," and that Numrich "is a highly ethical company and requires the highest standard of conduct from [its] employees and business partners." Exh. B.

37. Numrich represented to its online customers that their PCD would be secure. Plaintiffs and members of the proposed Class relied on such representations when they agreed to provide their PCD and transact with Numrich.

38. Consumers place value in data privacy and security. These are important considerations when deciding where to make certain purchases. Plaintiffs would not have transacted with, nor provided their PCD to Numrich had they known that Numrich does not take all necessary precautions to secure the personal and financial data given to it by consumers.

[6] See Numrich's Website: https://www.gunpartscorp.com/privacy (last visited June 15, 2022).

39. Despite its alleged commitments to securing sensitive customer data, Numrich does not follow industry standard practices in securing customers' PCD.

40. In January 2022, hackers bypassed Numrich's security safeguards and infiltrated its systems, giving them unfettered access to customers' PCD.

41. On information and belief, the Data Breach was undetected for at least 2 months.

42. In response to the Data Breach, Numrich contends that it "took steps to confirm the security of [its] systems . . . [and] worked quickly to secure [its] website and implement additional network and endpoint monitoring to reduce the risk of recurrence." Exh. A. These measures should have been in place *before* the Data Breach.

43. Numrich's Breach Notice omits the size and scope of the breach. Numrich has demonstrated a pattern of providing inadequate notices and disclosures about the Data Breach.

44. On information and belief, the Data Breach has impacted at least 45,169 former and current Numrich online customers.

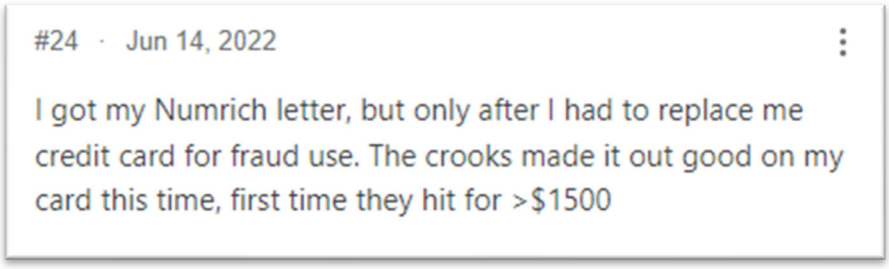
45. On information and belief, Numrich does not adequately train its employees on cybersecurity policies, enforce those policies, or maintain reasonable security practices and systems.

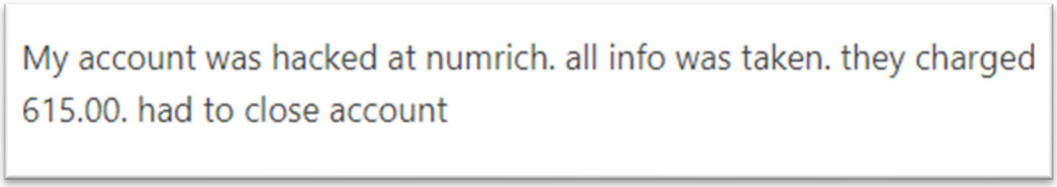
46. Numrich's negligent conduct caused the Data Breach. Numrich violated its obligation to implement best practices and comply with industry standards concerning website system security. Numrich failed to comply with security standards and allowed its customers' PCD to be accessed and stolen by failing to implement security measures that could have prevented, mitigated, or timely detected the Data Breach.

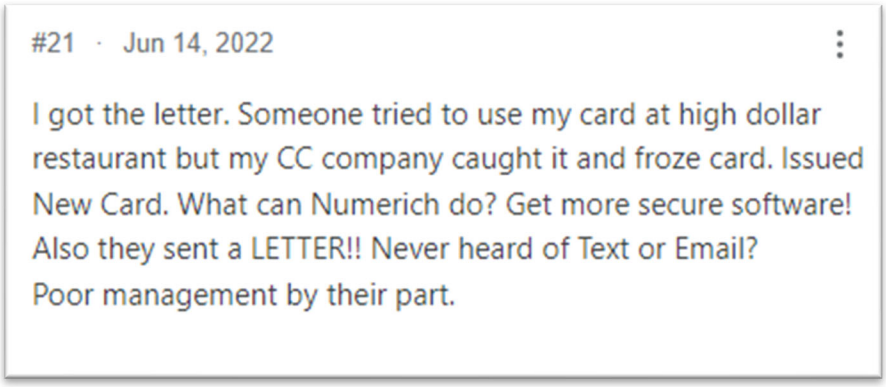
47. On information and belief, Numrich did not cease its online operations during the Breach Period and exposed the PCD of additional customers after discovering the Data Breach.

b. Fraud and Identity Theft Following Numrich's Breach

48. Consumers are already reporting rampant fraud and identity theft following Numrich's breach. Responding to those instances has required breach victims to remedy any fraud, cancel their card, and open new cards with their financial institutions:[7]







[7] *See* the forum posts at Gunboards.com (https://www.gunboards.com/threads/numrich-hacked.1223579/page-2 (last visited October 20, 2022)) and M14Forum (https://www.m14forum.com/threads/numrich-credit-card-hack.524692/page-2 (last visited October 20, 2022).

49. And these are only the publicly reported instances of fraud and identity theft following the breach.

50. Plaintiffs and the Class are thus justified in expending time and resources mitigating the threats to their accounts and identity, as cybercriminals have and will continue to misuse their data.

c. Plaintiffs' Experiences

Plaintiff Koeller

51. Plaintiff Koeller has been a Numrich customer since approximately 2015, making at least two purchases from Numrich's website, the most recent being on February 8, 2022.

52. As a condition of completing his online transactions, Plaintiff Koeller was required to provide his PCD to Numrich.

53. Plaintiff Koeller provided his PCD to Numrich and trusted that the company would use reasonable measures to protect it according to Numrich's Privacy Policy and state and federal law.

54. In mid-June 2022, Plaintiff Koeller received a notice letter from Numrich closely resembling the Breach Notice confirming Plaintiff Koeller's PCD was stolen as a result of the Data Breach.

55. In response to the Data Breach, and to learning about instances of payment card fraud affecting other Numrich customers, Plaintiff Koeller has devoted time and resources to canceling the payment card associated with his Numrich purchases and reviewing his accounts for fraud. In so doing, Plaintiff Koeller spent time reviewing the breach notice and public sources for the scope of the information lost in the Data Breach (10 minutes), his personal documents to determine which payment cards were associated with the breach (10 minutes), his account statements for any instances of fraud that may have occurred over since the Data Breach (45 minutes), and his credit reports for instances of fraud (45 minutes). Plaintiff Koeller also spent time contacting his card service provider to cancel his the card associate with his Numrich purchases (5 minutes) and then ordered a new card (5 minutes). While canceling his payment card, Plaintiff Koeller's payment card processer recommended that he review his account statements for fraudulent charges. Altogether, Plaintiff Koeller devoted around two hours to mitigating the harm associated with the Data Breach.

56. Further, Plaintiff Koeller will devote time to switching his account numbers with payment processers.

57. What's more, Plaintiff Koeller fears for his personal safety following the Data Breach. As a gun owner, Plaintiff Koeller is now at risk for burglary and theft due to the data

breach, as criminals know where he lives and that he owns guns. As a result, Plaintiff Koeller is experiencing feelings of anxiety, sleep disruption, stress, fear, and frustration because of the Data Breach. Numrich's Data Breach violated his privacy, and the harm it causes goes far beyond allegations of mere worry or inconvenience; it is exactly the sort of injury and harm to a Data Breach victim that the law contemplates and addresses.

Plaintiff Cheek

58. Plaintiff Cheek has been a Numrich customer since approximately 2017, making at least two purchases from Numrich's website, the most recent being approximately May of 2022.

59. As a condition of completing his online transactions, Plaintiff Cheek was required to provide his PCD to Numrich.

60. Plaintiff Cheek provided his PCD to Numrich and trusted that the company would use reasonable measures to protect it according to Numrich's Privacy Policy and state and federal law.

61. In mid-June 2022, Plaintiff Cheek received a notice letter from Numrich closely resembling the Breach Notice confirming Plaintiff Cheek's PCD was stolen as a result of the Data Breach.

62. When purchasing products from Numrich, Plaintiff Cheek used his Apple Card issued by Goldman Sachs. From approximately May 2022 through September 2022, and since the time of the Data Breach, Mr. Cheek has received approximately 15 different notices from Goldman Sachs regarding fraudulent transactions on his Apple card.

63. In response to the Data Breach, and to learning about instances of payment card fraud affecting other Numrich customers, Plaintiff Cheek has devoted time and resources to canceling the payment card associated with his Numrich purchases and reviewing his accounts for

fraud. In so doing, Plaintiff Cheek spent time reviewing the breach notice and public sources for the scope of the information lost in the Data Breach (15 minutes), his personal documents to determine which payment cards were associated with the breach (20 minutes), his account statements for any instances of fraud that may have occurred over since the Data Breach (45 minutes), and his credit reports for instances of fraud (45 minutes). Plaintiff Cheek also spent time repeatedly communicating with his card service provider to identify the fraud and cancel the card associated with his Numrich purchases (15 minutes) and then ordered a new card (5 minutes). Altogether, Plaintiff Cheek devoted in excess of two hours to mitigating the harm associated with the Data Breach.

64. Further, Plaintiff Cheek will devote time to switching his account numbers with payment processers.

65. What's more, Plaintiff Cheek fears for his personal safety following the Data Breach. As a gun owner, Plaintiff Cheek is now at risk for burglary and theft due to the data breach, as criminals know where he lives and that he owns guns. As a result, Plaintiff Cheek is experiencing feelings of anxiety, sleep disruption, stress, fear, and frustration because of the Data Breach. Numrich's Data Breach violated his privacy, and the harm it causes goes far beyond allegations of mere worry or inconvenience; it is exactly the sort of injury and harm to a Data Breach victim that the law contemplates and addresses.

d. Plaintiffs and the Proposed Class Suffered Damages

66. Plaintiffs and members of the proposed Class have suffered injury from the misuse of their PCD that can be directly traced to Defendant.

67. According to a 2020 Federal Trade Commission report, credit card fraud is the most

common type of identity theft.[8]

68. As a result of Numrich's failure to prevent the Data Breach, Plaintiffs and the proposed Class have suffered and will continue to suffer damages, including monetary losses, lost time, anxiety, and emotional distress. They have suffered or are at an increased risk of suffering:

a. The loss of the opportunity to control how their PCD is used;

b. The diminution in value of their PCD;

c. The compromise and continuing publication of their PCD;

d. Out-of-pocket costs associated with the prevention, detection, recovery, and remediation from identity theft or fraud;

e. Lost opportunity costs and lost wages associated with the time and effort expended addressing and attempting to mitigate the actual and future consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest, and recover from identity theft and fraud;

f. Unauthorized use of stolen PCD; and

g. The continued risk to their PCD, which remains in the possession of defendant and is subject to further breaches so long as defendant fails to undertake the appropriate measures to protect the PCD in their possession.

69. Stolen credit cards are considered highly valuable commodities on the criminal information black market. According to Forbes Advisor, a team of financial and economy journalists, a single consumer's stolen credit card information can be worth up to $150.00

[8]https://www.ftc.gov/system/files/documents/reports/consumer-sentinel-network-data-book-2019/consumer_sentinel_network_data_book_2019.pdf (last visited June 15, 2022).

depending on the type of supplementary information included.[9] Indeed, selling stolen credit card information in "bulk guarantees a lucrative payout—even if the fraud does not ultimately succeed."[10]

70. Payment card data breaches can have devastating and lasting impacts on breach victims. Criminals learn the victims' purchasing behaviors and habits, and can use this sensitive information to mimic the victims' behaviors to lower the chances of fraudulent charges getting caught by financial institutions and the breach victims themselves.[11]

71. It can take victims months or years to spot identity or PCD theft, giving criminals plenty of time to use that information for cash.

72. Criminals in possession of stolen credit card information can take over the victims' existing accounts, make fraudulent charges, and even open new accounts using the victims' personal financial information without their knowledge.[12]

73. That is exactly what is happening to Plaintiffs and members of the proposed Class, and it is reasonable for any trier of fact, including this Court or a jury, to find that Plaintiffs and other members of the proposed Class's stolen PCD is being misused, and that such misuse is fairly traceable to the Data Breach.

74. According to the FBI's Internet Crime Complaint Center (IC3) 2019 Internet Crime Report, Internet-enabled crimes reached their highest number of complaints and dollar losses that

---

[9] *What Happens to Stolen Credit Card Numbers?,* Forbes.com (Apr. 19, 2022), https://www.forbes.com/advisor/credit-cards/what-happens-to-stolen-credit-card-numbers/#:~:text=A%20single%20consumer's%20stolen%20credit%20information%20card%20sells,value%20of%20the%20card%2C%20but%20not%20by%20much (last visited June 15, 2022).

[10] *Id.*

[11] *Id.*

[12] *15 Disturbing Credit Card Fraud Statistics*, Cardrates.com (Mar. 16, 2022), https://www.cardrates.com/advice/credit-card-fraud-statistics/ (last visited June 15, 2022).

year, leading to more than $3.5 billion in losses to individuals and business victims.[13]

75. Further, "rapid reporting can help law enforcement stop fraudulent transactions before a victim loses the money for good."[14] Defendant did not rapidly report to Plaintiffs and the Class that their PDC had been stolen.

76. Victims of identity theft also often suffer embarrassment, blackmail, or harassment in person or online, and experience financial losses resulting from fraudulently opened accounts or misuse of existing accounts.

77. In addition to out-of-pocket expenses that can exceed thousands of dollars for the victim of new account identity theft, and the emotional toll identity theft can take, some victims have to spend a considerable time repairing the damage caused by the theft of their PCD. Victims of new account identity theft will likely have to spend time correcting fraudulent information in their credit reports and continuously monitor their reports for future inaccuracies, close existing bank/credit accounts, open new ones, and dispute charges with creditors.

78. Further complicating the issues faced by victims of identity theft, data thieves may wait years before attempting to use the stolen PCD. To protect themselves, Plaintiffs and the Class will need to be remain vigilant against unauthorized data use for years to come.

79. Defendant disclosed the PCD of Plaintiffs and members of the proposed Class for criminals to use in the conduct of criminal activity. Specifically, Defendant opened up, disclosed, and exposed the PCD of Plaintiffs and members of the proposed Class to people engaged in disruptive and unlawful business practices and tactics, including online account hacking,

---

[13] *2019 Internet Crime Report Release*, fbi.gov (Feb. 11, 2020), https://www.fbi.gov/news/stories/2019-internet-crime-report-released-021120#:~:text=The%20Importance%20of%20Reporting,-"Information%20reported%20to&text=Rapid%20reporting%20can%20help%20law,to%20build%20on%20its%20success. (last visited June 15, 2022).

[14] *Id.*

unauthorized use of financial accounts, and fraudulent attempts to open unauthorized financial accounts (i.e., identity fraud), all using the stolen PCD.

80. Defendant's use of outdated and insecure computer systems and software that are easy to hack, and its failure to maintain adequate security measures and an up-to-date technology security strategy, demonstrates a willful and conscious disregard for privacy, and has exposed the PCD of Plaintiffs and potentially thousands of members of the proposed Class to unscrupulous operators, con artists and outright criminals.

81. Defendant's failure to properly notify Plaintiffs and members of the proposed Class of the Data Breach exacerbated Plaintiffs' and members of the proposed Class's injury by depriving them of the earliest ability to take appropriate measures to protect their PCD and take other necessary steps to mitigate the harm caused by the Data Breach.

82. Further, as Plaintiffs allege above, the Data Breach violates Plaintiffs' and the Class's privacy and poses a continuing risk to their safety.

83. Just as criminals can misuse the PCD to steal Plaintiffs and the Class's identities and commit fraud, they can use it to target individuals they know own valuable guns.

84. Indeed, state officials in California are confronting a similar threat. There, a state agency lost control over the gun ownership data relating to thousands of Californians registered with the state's concealed carry program.[15]

85. In that instance, state officials recognize the breach's victims are at risk: "'It is infuriating that people who have been complying with the law have been put at risk by this breach,' said Butte County Sheriff Kory Honea, the [California State Sheriffs' Assn.]'s president.

[15] *See* the California Department of Justice alert at https://oag.ca.gov/news/press-releases/california-department-justice-alerts-individuals-impacted-exposure-personal (last visited Oct. 20, 2022).

'California's sheriffs are very concerned about this data breach and the risk it poses to California's CCW permit holders.'"[16]

86. Plaintiffs and the Class are at the same risk here and they cannot eliminate that safety risk by merely canceling affect payment card accounts.

CLASS ACTION ALLEGATIONS

87. Plaintiffs bring this action pursuant to Federal Rule of Civil Procedure 23 on behalf of themselves and all members of the proposed class (the "Class"), defined as follows:

> All persons in the United States whose personal and financial information was compromised in the Data Breach disclosed by Numrich in June 2022.

88. The following people are excluded from the Class: (1) any judge or magistrate presiding over this action and members of their families; (2) Defendant, Defendant's subsidiaries, parents, successors, predecessors, affiliated entities, and any entity in which Defendant or its parent has a controlling interest, and their current or former officers and directors; (3) persons who properly execute and file a timely request for exclusion from the Class; (4) persons whose claims in this matter have been finally adjudicated on the merits or otherwise released; (5) Plaintiffs' counsel and Defendant's counsel; and (6) the legal representatives, successors, and assigns of any such excluded persons

89. Plaintiffs reserve the right to amend the Class definition or add a Class if further information and discovery indicate that other classes should be added and if the definition of the Class should be narrowed, expanded, or otherwise modified.

[16] *See* the article "Leak of California concealed-carry permit data is larger than initially reported" at https://www.latimes.com/california/story/2022-06-29/california-concealed-carry-weapons-permit-data-exposed-in-leak (last visited Oct. 20, 2022).

90. This action satisfies the numerosity, commonality, typicality, and adequacy requirements under Fed. R. Civ. P. 23.

a. **Numerosity**. Plaintiffs is representative of the proposed Class, consisting of thousands of members, far too many to join in a single action;

b. **Ascertainability**. Class members are readily identifiable from information in Defendant's possession, custody, and control;

c. **Typicality**. Plaintiff's claims are typical of Class member's claims as each arises from the same Data Breach, the same alleged violations by Defendant, and the same unreasonable manner of notifying individuals about the Data Breach;

d. **Adequacy**. Plaintiffs will fairly and adequately protect the proposed Class's interests. Plaintiff's interests do not conflict with Class members' interests and Plaintiffs has retained counsel experienced in complex class action litigation and data privacy to prosecute this action on the Class's behalf, including as lead counsel Defendant has no defenses unique to Plaintiffs.

e. **Commonality**. Plaintiffs' and the Class's claims raise predominantly common fact and legal questions that a class wide proceeding can answer for all Class members. Common questions for the Class include, but are not necessarily limited to the following:

i. Whether Defendant had a duty to use reasonable care in safeguarding Plaintiffs' and the Class's PCD;

ii. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

iii. Whether Defendant was negligent in maintaining, protecting, and securing PCD;

iv. Whether Defendant breached contract promises to safeguard Plaintiffs and the Class's PCD;

v. Whether Defendant took reasonable measures to determine the extent of the Data Breach after discovering it;

vi. Whether Defendant's Breach Notice was reasonable;

vii. Whether the Data Breach caused Plaintiffs and the Class injuries;

viii. What the proper damages measure is; and

ix. Whether Plaintiffs and the Class are entitled to damages, treble damages, or injunctive relief.

91. Further, common questions of law and fact predominate over any individualized questions, and a class action is superior to individual litigation or any other available method to fairly and efficiently adjudicate the controversy. The damages available to individual plaintiffs are insufficient to make individual lawsuits economically feasible.

COUNT I
Negligence
(On Behalf of Plaintiffs and the Class)

92. Plaintiffs and members of the Class incorporate all previous paragraphs as if fully set forth herein.

93. Plaintiffs and members of the Class entrusted their PCD to Defendant. Upon accepting and storing Plaintiffs' and members of the Class's PCD in its database system, Defendant undertook and owed to Plaintiffs and other members of the Class a duty to exercise reasonable care in handling and using the PCD in its care and custody, including implementing

industry-standard security procedures sufficient to reasonably protect the information from the Data Breach, theft, and unauthorized use that came to pass, and to promptly detect attempts at unauthorized access.

94. Defendant owed a duty of care to Plaintiffs and members of the Class because it was foreseeable that Defendant's failure to adequately safeguard their PCD in accordance with state-of-the-art industry standards concerning data security would result in the compromise of that PCD —just like the Data Breach that ultimately came to pass. Defendant acted with wanton and reckless disregard for the security and confidentiality of Plaintiffs' and members of the Class's PCD by disclosing and providing access to this information to third parties and by failing to properly supervise both the way the PCD was stored, used, and exchanged, and those in its employ who were responsible for making that happen.

95. Defendant owed to Plaintiffs and members of the Class a duty to notify them within a reasonable timeframe of any breach to the security of their PCD. Defendant also owed a duty to timely and accurately disclose to Plaintiffs and members of the Class the scope, nature, and occurrence of the Data Breach. This duty is required and necessary for Plaintiffs and members of the Class to take appropriate measures to protect their PCD, to be vigilant in the face of an increased risk of harm, and to take other necessary steps to mitigate the harm caused by the Data Breach.

96. Defendant owed these duties to Plaintiffs and members of the Class because they are members of a well-defined, foreseeable, and probable class of individuals whom Defendant knew or should have known would suffer injury-in-fact from Defendant's inadequate security protocols. Defendant actively sought and obtained Plaintiffs' and members of the Class's personal information and PCD.

97. The risk that unauthorized persons would attempt to gain access to the PCD and misuse it was foreseeable. Given that Defendant holds vast amounts of PCD, it was inevitable that unauthorized individuals would attempt to access Defendant's databases containing the PCD — whether by malware or otherwise.

98. PCD is highly valuable, and Defendant knew, or should have known, the risk in obtaining, using, handling, emailing, and storing the PCD of Plaintiffs and members of the Class's and the importance of exercising reasonable care in handling it, particularly given the privacy concerns implicated by gun ownership and the threat to physical safety that can result by gun ownership being publicized.

99. Defendant breached its duties by failing to exercise reasonable care in supervising its agents, contractors, vendors, and suppliers, and in handling and securing the personal information and PCD of Plaintiffs and members of the Class which actually and proximately caused the Data Breach and Plaintiffs' and members of the Class's injury. Defendant further breached its duties by failing to provide reasonably timely notice of the Data Breach to Plaintiffs and members of the Class, which actually and proximately caused and exacerbated the harm from the Data Breach and Plaintiffs' and members of the Class's injuries-in-fact.

100. As a direct and traceable result of Defendant's negligence and/or negligent supervision, Plaintiffs and members of the Class have suffered or will suffer damages, including, but not limited to: monetary damages arising from unauthorized charges on their debit or credit cards or on cards that were fraudulently obtained through the use of the stolen PCD and/or filing false tax returns; damages from identity theft, which may take months, if not years, to discover and detect, given the far-reaching, adverse, and detrimental consequences of identity theft and loss of privacy; loss of time spent addressing the present and ongoing risk of identity theft and financial

fraud; and embarrassment, humiliation, frustration, emotional distress, and concern for their own personal safety. The nature of other forms of economic damage and injury may take years to detect and the potential scope can only be assessed after a thorough investigation of the facts and events surrounding the theft of PCD described above.

COUNT II
Breach of Implied Contract
(On Behalf of Plaintiffs and the Class)

101. Plaintiffs and members of the Class incorporate all previous paragraphs as if fully set forth herein.

102. Defendant solicited Plaintiffs and members of the Class to purchase firearms parts through its website using their credit or debit cards. Plaintiffs and members of the Class accepted Defendant's offers and used their credit or debit cards to purchase goods from Defendant's website during the period of the Data Breach.

103. When Plaintiffs and members of the Class made and paid for purchases, they provided their PCD by entering their credit or debit card numbers/information into the Defendant's website. In doing so, Plaintiffs and members of the Class entered into implied contracts with Defendant pursuant to which Defendant agreed to safeguard and protect such information and to timely and accurately notify Plaintiffs and members of the Class if their data had been breached and compromised.

104. Each purchase on the Defendant's website during the Data Breach period was made pursuant to the mutually agreed-upon implied contract with Defendant under which Defendant agreed to safeguard and protect Plaintiffs' and members of the Class's PCD and to timely and accurately notify Plaintiffs and members of the Class if such information was compromised or stolen.

105. Plaintiffs and the members of the Class would not have provided and entrusted their PCD to Defendant to make purchases through the website in the absence of the implied contract between them and Numrich.

106. Defendant materially breached the contract(s) it had entered with Plaintiffs and members of the Class by failing to safeguard and protect the PCD and by failing to notify Plaintiffs and members of the Class promptly of the intrusion into its website system that compromised such information. Defendant further breached the implied contracts with Plaintiffs and members of the Class by:

a. Failing to properly safeguard and protect Plaintiffs' and members of the Class's PCD;

b. Failing to comply with industry standards as well as legal obligations that are necessarily incorporated into the parties' agreement; and

c. Failing to ensure the confidentiality and integrity of electronic PCD that Defendant created, received, maintained, and transmitted.

107. The damages sustained by Plaintiffs and members of the Class as described above were the direct and proximate result of Defendant's material breaches of its agreement(s).

108. Plaintiffs and members of the Class have performed as required under the relevant agreements, or such performance was waived by the conduct of Defendant.

109. The covenant of good faith and fair dealing is an element of every contract. All such contracts impose upon each party a duty of good faith and fair dealing. The parties must act with honesty in fact in the conduct or transactions concerned. Good faith and fair dealing, in connection with executing contracts and discharging performance and other duties according to their terms, means preserving the spirit—not merely the letter—of the bargain. Put differently, the

parties to a contract are mutually obligated to comply with the substance of their contract in addition to its form.

110. Subterfuge and evasion violate the obligation of good faith in performance even when an actor believes their conduct to be justified. Bad faith may be overt or may consist of inaction, and fair dealing may require more than honesty.

111. Defendant failed to advise Plaintiffs and members of the Class of the Data Breach promptly and sufficiently.

112. In these and other ways, Defendant violated its duty of good faith and fair dealing.

113. Plaintiffs and members of the Class have sustained damages because of Defendant's breaches of its agreement, including breaches thereof through violations of the covenant of good faith and fair dealing.

COUNT III
Unjust Enrichment
(On Behalf of Plaintiffs and the Class)

114. Plaintiffs and members of the Class incorporate all previous paragraphs as if fully set forth herein.

115. This claim is pleaded in the alternative to the breach of implied contractual duty claim.

116. Plaintiffs and members of the Class conferred a benefit upon Defendant in the form of payments through Defendant's website.

117. Defendant appreciated or had knowledge of the benefits conferred upon itself by Plaintiffs and members of the Class. Defendant also benefited from the receipt of Plaintiffs and members of the Class's PCD, as this was used to facilitate their purchases.

118. Under principals of equity and good conscience, Defendant should not be permitted

to retain the full value of Plaintiffs' and the proposed Class's payments and their PCD because Defendant failed to adequately protect their PCD. Plaintiffs and the proposed Class would not have provided their PCD had they known Defendant would not adequately protect their PCD.

119. Defendant should be compelled to disgorge into a common fund for the benefit of Plaintiffs and members of the Class all unlawful or inequitable proceeds received by it because of its misconduct and Data Breach.

COUNT IV
Violation of the New York General Business Law, N.Y. Gen. Bus. Law § 349 *et seq.*
(On Behalf of Plaintiffs and the Class)

120. Plaintiffs and members of the Class incorporate all previous paragraphs as if fully set forth herein.

121. New York General Business Law § 349 ("GBL § 349") prohibits deceptive acts or practices in the conduct of any business, trade or commerce or in the furnishing of any service in the state of New York.

122. As a well-known firearm parts retailer, Numrich conducted business, trade, or commerce in New York State.

123. In the conduct of its business, trade and commerce, and in furnishing retail services in New York State, Numrich's actions were directed at consumers.

124. In the conduct of its business, trade and commerce, and in furnishing retail services in New York State, Numrich collected and stored highly personal and private financial information, including PCD belonging to Plaintiffs and members of the Class.

125. In the conduct of its business, trade and commerce, and in furnishing retail services in New York State, Numrich engaged in deceptive, unfair, and unlawful trade acts or practices, in violation of GBL § 349, including but not limited to the following:

a. Numrich misrepresented and fraudulently advertised material facts, pertaining to the sale and/or trading of firearms parts to Plaintiffs and the members of the Class that it would maintain adequate data privacy and security practices and procedures to safeguard its E-commerce customers' PCD from unauthorized sharing, disclosure, release, sell, or trade, and moreover, that its employees and business partners would do the same;

b. Numrich misrepresented material facts, pertaining to the sale and/or trading of firearm parts, to Plaintiffs and the members of the proposed Class by representing and advertising that it did and would comply with requirements of relevant federal and state laws pertaining to privacy and security of its E-commerce customers' PCD, and that its employees and business partners would do the same;

c. Numrich omitted, suppressed, and concealed the material facts of the Data Breach and its privacy and security protections for its E-commerce customers' PCD during the Breach Period—even after discovering the Data Breach;

d. Numrich engaged in deceptive, unfair, and unlawful trade acts or practices by failing to maintain the privacy and security of the Class's PCD, in violation of duties imposed by and public policies reflected in applicable federal and state laws, resulting in the Data Breach. These unfair acts and practices violated duties imposed by laws including the Federal Trade Commission Act (15. U.S.C. § 45);

e. Numrich engaged in deceptive, unfair, and unlawful trade acts or practices by failing to disclose the Data Breach to the Plaintiffs and members of the proposed Class "in the most expedient time possible and without unreasonable delay," contrary to the duties imposed by N.Y. Gen. Bus. Law § 899-aa(2); and

f. Numrich engaged in deceptive, unfair, and unlawful trade acts or practices by failing to take proper action following the Data Breach to enact adequate privacy and security measures to protect the Class's PCD from further unauthorized disclosure, release, data breaches, and theft.

126. Numrich systematically engaged in these deceptive, misleading, and unlawful acts and practices, to the detriment of the Plaintiffs and members of the proposed Class.

127. Numrich willfully engaged in such acts and practices, and knew it violated GBL § 349 or showed reckless disregard for whether it violated GBL § 349.

128. As a direct and proximate result of Numrich's deceptive trade practices, the Plaintiffs and members of the proposed Class suffered injury and/or damages, including the loss of their legally protected interest in the confidentiality and privacy of their PCD, and the loss of the benefit of their respective bargains.

129. The above unfair deceptive practices and acts committed by Numrich were unscrupulous, unethical, immoral, and oppressive. These acts caused substantial injury to Numrich's E-commerce customers that these consumers could not reasonably avoid. The substantial injuries outweighed any benefits to Numrich's E-commerce customers or to competition.

130. Numrich knew or should have known that its computer systems and data security practices were inadequate to safeguard the Plaintiffs' and members of the proposed Class's PCD and that risk of a data breach or cyber-attack were highly likely and foreseeable. Numrich's actions in engaging in the above-referenced unfair practices and deceptive acts were negligent, knowing, and willful, and/or wanton and reckless with respect to the rights of the Plaintiffs and members of the proposed Class.

131. Plaintiffs and members of the Class seek relief under GBL § 349(h), including, but not limited to, actual damages, treble damages, statutory damages, injunctive relief, and/or attorney's fees and costs.

PRAYER FOR RELIEF

Plaintiffs and members of the Class demand a jury trial on all claims so triable and request that the Court enter an order:

A. Certifying this case as a class action on behalf of Plaintiffs and the proposed Class, appointing Plaintiffs as class representatives, and appointing their counsel to represent the Class;

B. Awarding declaratory and other equitable relief as is necessary to protect the interests of Plaintiffs and the Class;

C. Awarding injunctive relief as is necessary to protect the interests of Plaintiffs and the Class;

D. Enjoining Defendant from further deceptive practices and making untrue statements about the Data Breach and the stolen PCD;

E. Awarding Plaintiffs and the Class damages that include applicable compensatory, exemplary, punitive damages, and statutory damages, as allowed by law;

F. Awarding restitution and damages to Plaintiffs and the Class in an amount to be determined at trial;

G. Awarding attorneys' fees and costs, as allowed by law;

H. Awarding prejudgment and post-judgment interest, as provided by law;

I. Granting Plaintiffs and the Class leave to amend this complaint to conform to the evidence produced at trial; and

J. Granting such other or further relief as may be appropriate under the circumstances.

JURY TRIAL DEMANDED

Plaintiffs hereby demand a trial by jury on all issues so triable.

Dated: November 16, 2022

Respectfully submitted,

By: */s/ Raina C. Borrelli*

Raina C. Borrelli
raina@turkestrauss.com
Samuel J. Strauss
sam@turkestrauss.com
Alex Phillips
alexp@turkestrauss.com
TURKE & STRAUSS LLP
613 Williamson St., Suite 201
Madison, WI 53703
Telephone (608) 237-1775
Facsimile: (608) 509-4423

James J. Bilsborrow
James J. Bilsborrow (NY Bar # 519903)
WEITZ & LUXENBERG, PC
700 Broadway
New York, NY 10003
Tel: 212-558-5500
Email: jbilsborrow@weitzlux.com

Attorneys for Plaintiffs and the Proposed Class